

橢圓曲線版的ElGamal 數位簽署

林文儀* 沈淵源*

Abstract

本研究的主要目的在探討橢圓曲線版的數位簽署，以及同步進行加密且簽署的過程。在此研究當中，首先提到有關 ElGamal 密碼系統及數位簽署的探討，接著論及有關橢圓曲線密碼系統。本研究最後採用 ElGamal 加密及簽署的概念，並將其修飾而成爲橢圓曲線版的 ElGamal 數位簽署，且加以改良後，推出同步進行加密且簽署的過程。

1 ElGamal 密碼系統

ElGamal於一九八五年所提出的密碼系統 [1]。因爲密文不僅僅與明文有關，而且跟加密者在加密時所選取的隨機整數有關。所以同一明文就會產生許許多多不同的密文。

假設 B 要傳遞信息 m 給 A 。首先 A 選取一個大質數 p 及一個整數 $\alpha \pmod{p}$ ，同時 A 也選取一私密整數 a 並計算 $\beta \equiv \alpha^a \pmod{p}$ 。 A 將 (p, α, β) 公開，但將 a 把持私密。 B 則根據 A 所公開的鑰匙，選取一隨機整數 k 並算出 y_1 與 y_2 ，此處

$$y_1 \equiv \alpha^k, \quad y_2 \equiv m\beta^k \pmod{p}$$

B 將密文 y_1, y_2 送出給 A ，然後 A 據此解密如下：

$$m \equiv y_2 y_1^{-a} \pmod{p}$$

2 ElGamal 的數位簽署

假設 A 要簽署一份文件 m 。首先他選擇一個大質數 p 及一個原根 α ，然後選取一個介於 1 與 $p-2$ 之間的整數 a 並且計算 $\beta \equiv \alpha^a \pmod{p}$ 。其公開的參數爲 p, α 和 β 。整個系統的安全性完全是建立在 a 的私密性上。敵對者想從 (p, α, β) 來決定是困難重重的，因爲離算對數問題被認爲是困難的。 A 要簽署一信息 m ，他可以進行如下得到簽署文 (m, r, s) ：

*東海大學數學系

1. 選取一秘密隨機整數 k 使得 $\gcd(k, p-1) = 1$ 。
2. 計算 $r \equiv \alpha^k \pmod{p}$ 。
3. 計算 $s \equiv k^{-1}(m - ar) \pmod{p-1}$ 。
4. 簽署後的信息為 (m, r, s) 。

B 可以驗證此簽名的有效性, 其步驟如下:

1. 下載 A 的公開鑰匙 (p, α, β) 。
2. 計算 $v_1 \equiv \beta^r r^s \pmod{p}$ 以及 $v_2 \equiv \alpha^m \pmod{p}$ 。
3. 接受此為有效簽名 $\iff v_1 = v_2$ 。

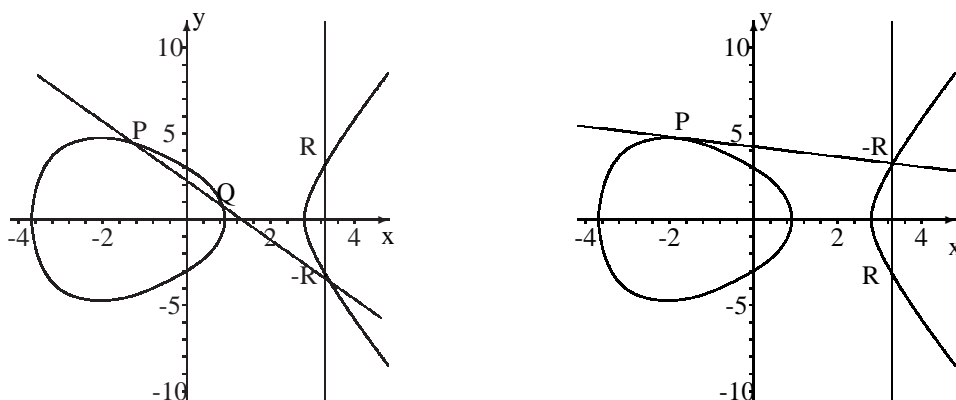
3 橢圓曲線與密碼系統

在一八九零年代的中期, 米勒 (Miller[3]) 與寇伯立茲 (Koblitz[4]) 將橢圓曲線引進密碼術 (Cryptograph) 當中, 而藍斯特 (Lenstra[5]) 則指出如何使用橢圓曲線來分解因數。從此開始, 橢圓曲線在密碼學的許多地方扮演著一個重要的角色。優點之一是與傳統密碼系統使用相當大的鑰匙來比較, 橢圓曲線看起來似乎提供了某種程度的安全水準。

下列的方程式我們稱之為橢圓曲線

$$E: y^2 = x^3 + ax + b$$

此處的 a, b 佈於任合適用的集合如有理數、實數、負數、模 p 之下之整數或有限數體。在任何的橢圓曲線的定義中都有一個元素 ∞ , 稱之為「無限遠點 (Point at infinity) 或零點 (Zero point)」。此無限遠點最簡單的一個處理方式就是將此點看作在 y -軸的最上方。這可以放在投影幾何的背景下嚴密地處理, 但上面直觀的概念對我們來講已足夠了。我們可以參考 Silverman 與 Tate 二人所合寫的書《橢圓曲線上的有理點 (Rational Points On Elliptic Curves[8])》若將 y -軸最下方的點看成是最上方的點。則 ∞ 也是位於 y -軸的最下方。在實數的領域下, 圖形只有兩種可能的形式, 就是看右邊那個的三次多項式有三個相異的實根或是一個實根而定。重根的情況又另當別論, 通常我們假設三次多項式 $x^3 + ax + b$ 沒有重根。請參考下面之圖形。



橢圓曲線 $y^2 = x^3 - 10x + 10$ 上 $P + Q = R$ 橢圓曲線 $y^2 = x^3 - 10x + 10$ 上 $P + P = R$

4 橢圓曲線上的加法律

對橢圓曲線加密系統 (Elliptic Curves Cryptosystem) 而言, 我們所關心的是在有限體內的橢圓曲線。在密碼學上特別的是取 p 的同餘的橢圓曲線, 此處 p 為質數。其定義如下: 挑選兩個小於 p 的非負整數, 滿足

$$4a^3 + 27b^2 \pmod{p} \neq 0$$

則 $E_p(a, b)$ 表示取 p 的同餘的橢圓曲線, 其元素 (x, y) 是一對小於 p 的非負整數, 滿足

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

, 以及無限遠點 ∞ 。因此對橢圓曲線來說, 我們只對 $(0, 0)$ 到 (p, p) 間滿足方程式 (取 p 之同餘) 的非負整數點有興趣。通常這些點可由下列方式列出:

1. 對每個滿足 $0 \leq x < p$ 的 x 來說, 計算 $x^3 + ax + b \pmod{p}$ 。
2. 檢查上一步所產生的結果是否有平方根 (取 p 的同餘)[6]。如果沒有的話則 $E_p(a, b)$ 沒有此 x 的點。如果有的話, 會有兩個平方根 y (除非此 y 值為 0)。這些 (x, y) 值為 $E_p(a, b)$ 上的點。

$E_p(a, b)$ 上的加法規則與圖上的幾何技巧是相對應的。對所有的點 $P, Q \in E_p(a, b)$ 來說, 其加法如下:

1. ∞ 為加法單位元素。因此 $\infty = -\infty$; 對任何在橢圓曲線上的點 P 而言, $P + \infty = P$ 。
2. 垂直線會和曲線相交於兩點, 這兩點具有相同的 x 座標, 如果 $P = (x, y)$, 則 $P + (x, -y) = \infty$ 。點 $(x, -y)$ 為負 P , 記為 $-P$ 。請注意 $(x, -y)$ 為橢圓曲線上的點 (也就是在 $E_p(a, b)$ 上)。所以一點的負點會有相同的 x 座標, 但是 y 座標變成負的。其圖說明此性質。

3. 給予不同 x 座標的兩點 P 及 Q 相加的話。可得到在橢圓曲線上的第三點如下：經過 P 及 Q 二點畫一直線 L (若 $P = Q$, 則取切線)。直線 L 與橢圓曲線交於 R , 然後求其 x -軸的對稱點 $-R$ (亦即 y 座標變號), 亦即 $P + Q + R = \infty$ 且 $P + Q = -R$ 。其圖說明此性質。
4. 令 $P = (x_1, y_1), Q = (x_2, y_2)$ 為橢圓曲線上之兩點, 並且 $P \neq Q$, 則 $P + Q = (x_3, y_3)$ 。此處

$$x_3 \equiv m^2 - x_1 - x_2 \pmod{p}$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \pmod{p}$$

其中的 m 為

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & , \text{ if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & , \text{ if } P = Q \end{cases}$$

我們來看下列的例子：考慮在模 5 之下的橢圓曲線

$$E : y^2 \equiv x^3 + 2x + 3 \pmod{5}$$

滿足 $E_5(2, 3)$ 的點為 $(1, 1), (1, 4), (2, 0), (3, 1), (3, 4), (4, 0)$ 及 ∞ 。令 $P = (1, 4)$ 且 $Q = (3, 1)$, 則 $m \equiv \frac{1-4}{3-1} \equiv 1 \pmod{5}$ 。

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 1^2 - 1 - 3 \equiv 2 \pmod{5}$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \equiv 1(1 - 2) - 4 \equiv 0 \pmod{5}$$

亦即 $P + Q = (2, 0)$ 。若要計算 $2P = P + P$ 的話, 則求其切線斜率 $\frac{dy}{dx}$ 在點 $P = (1, 4)$ 的值如下:

$$m \equiv \frac{3x_1^2 + a}{2y_1} \equiv \frac{3(1)^2 + 2}{2(4)} \equiv \frac{5}{8} \equiv \frac{0}{3} \equiv 0 \pmod{5}$$

並由公式得到

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 0^2 - 1 - 3 \equiv 1 \pmod{5}$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \equiv 0(1 - 2) - 4 \equiv 1 \pmod{5}$$

後的答案則是 $2P = (0, 1)$ 。

上述的加法規則滿足一般加法特性, 像交換性與結合性。橢圓曲線上一點 P 乘上一整數 k 的定義, 就像把 P 加 k 次一樣。因此, $2P = P + P$, $3P = P + P + P$, 以此類推。

5 如何用橢圓曲線上的點來表示明文?

將明文信息編碼而成爲橢圓曲線上的點的問題,並不像傳統的情況那樣簡單。這裡有一個 Koblitz 的方法。其想法如下:令 $E: y^2 \equiv x^3 + ax + b \pmod{p}$ 爲一橢圓曲線。已經數字化的信息 m 將看成是這橢圓曲線上的某一點的 x 座標。然而 $m^3 + am + b$ 在模 p 之下是平方數的概率至少 $1/2$ 。因此我們在 m 後面接上一個位元成爲另一個數,稱之爲 x ,藉著調整此位元直到我們得到一個 x 使得 $x^3 + ax + b$ 在模 p 之下爲平方數。

更明確地說,令 K 爲一個大整數使得將信息編碼成爲橢圓曲線上的點時,其失敗率爲 $1/2^K$ 是可接受的。假設 m 滿足 $(m+1)K < p$,將此信息 m 表示成一個形如 $x = mK + j$ 的數,此數 $0 \leq j \leq K$ 。對 $j = 0, 1, \dots, K-1$,計算 $x^3 + ax + b$ 並計算在模 p 之下的平方根。若有一平方根 y ,則取 $P_m = (x, y)$,否則將 j 增加 1 形成新的 x ,然後重複上述的步驟。如此這般地,直等到找著了一個平方根或是 $j = K$ 。如果 j 總是等於 K ,那麼對這個信息而言,我們的任務就無法達成。因爲 $x^3 + ax + b$ 大約有一半的時間是一個平方數,所以我們大約有 $1/2^K$ 失敗的機會。

由點 $P_m = (x, y)$,如何回復到原信息呢?僅需計算 $\frac{x}{K}$,取其整數部分即可。所以 $m = \lfloor \frac{x}{K} \rfloor$,此處 $\lfloor \frac{x}{K} \rfloor$ 爲高斯符號,就是小於或等於 $\frac{x}{K}$ 的最大整數。

例題:

令 $p = 179$ 且假設我們的橢圓曲線爲 $y^2 = x^3 + 2x + 7$ 。若可以接受 $1/2^{10}$ 的失敗率,則取 $K = 10$ 。因爲我們要求 $(m+1)K < 179$,故 $0 \leq m \leq 16$ 。假設我們的信息爲 $m = 5$ 。考慮形如 $mK + j = 50 + j$ 的 m 值,可能的選擇爲 $50, 51, \dots, 59$ 。對 $x = 51$,我們得到

$$x^3 + 2x + 7 \equiv 121 \pmod{179}, 11^2 \equiv 121 \pmod{179}$$

因此我們用點 $P_m = (51, 11)$ 來表示信息 $m = 5$ 。因此信息 m 可還原如下: $m = \lfloor \frac{51}{11} \rfloor = 5$ 。

6 橢圓曲線加密法

已有文獻分析了現有的數種橢圓曲線的加解密方法。在這裡,讓我們來看看最簡單的一種。首先系統將要送的明文 m 編碼成橢圓曲線上的點 P_m 。點 P_m 會被加密成密文,並且稍後會被解密。要注意的是我們不能單純地將信息編碼成某個點的 x 或 y 座標,因爲並不是所有的這類座標都會在 $E \pmod{p}$ 上。在一個鑰匙交換系統中,其加解密系統需要兩個參數, α 和橢圓曲線 $E \pmod{p}$ 。

首先,使用者 A 選擇一私密鑰匙 a_A ,然後再產生一公開鑰匙 $\beta_A = a_A \alpha$ 。同樣地使用者 B 也選擇一私密鑰匙 a_B ,然後再產生一公開鑰匙 $\beta_B = a_B \alpha$ 。

爲了將加密後的信息 P_m 傳送給 B , A 選擇一隨機正整數 k ,並且產生一個由兩個點所組成的密文 C_m 。

$$C_m = \{k\alpha, P_m + k\beta_B\}$$

請注意, A 用的是 B 的公開鑰匙 β_B 。為了解開密文, B 用自己的私密鑰匙乘上第一點, 再用第二點減去得到的結果, 可得

$$P_m + k\beta_B - a_B(k\alpha) = P_m + k(a_B\alpha) - a_B(k\alpha) = P_m$$

A 藉由加上 $k\beta_B$ 來隱藏訊息 P_m 。除了 A 之外沒人知道 k 的值, 所以即使 β_B 是公開的鑰匙, 也沒人能移除隱藏用的 $k\beta_B$ 。然而, A 在信息中加入了移除隱藏的「線索」, 如果有人知道私密鑰匙 a_B 的話, 就可以移除 $k\beta_B$ 。給定 α 和 $k\alpha$, 攻擊者必須計算出才能破解, 但這是很困難的。

此方法有可能不是很實用, 但我們也可以用 Menezes-Vanstone[2] 方法來做加密, 因為此方法在加密時不需先將信息 m 轉換成橢圓曲線上的點即可做加密的動作。

例題:

考慮在模 179 之下的橢圓曲線

$$E : y^2 \equiv x^3 + 2x + 7 \pmod{179}$$

並在其上選取一點 $\alpha = (111, 11)$ 再將此 $(111, 11)$ 及橢圓曲線 $E_{179}(2, 7)$ 公開。使用者 A 選取一私密鑰匙 $a_A = 12$, 然後 A 產生一公開鑰匙 $\beta_A \equiv 12 * (111, 11) = (111, 168) \pmod{179}$ 。使用者 B 同樣地選擇一私密鑰匙 $a_B = 9$, 並且計算其公開鑰匙 $\beta_B \equiv 9 * (111, 11) = (20, 23) \pmod{179}$ 。

若 A 要將信息 $m = 5$ 加密後傳送給 B , 其進行步驟如下:

1. 欲傳送信息 $m = 5$, 所以選擇 $K = 10$ 。可以成功的將 m 轉換成爲 $x = 5 * 10 + 1 = 51, y = 11$ 的點 $P_m = (51, 11)$ 。
2. 選取隨機整數 $k = 11$ 。
3. 計算 $y_1 \equiv k\alpha \equiv (152, 26) \pmod{179}$
4. 計算 $y_2 \equiv P_m + k\beta_B \equiv (156, 18) \pmod{179}$

因此 A 所產生的密文 $C_m = \{(152, 26), (156, 18)\}$ 。 B 可由 A 所產生的密文 C_m 來加以解密: 計算

$$y_2 - a_B y_1 \equiv P_m + k\beta_B - a_B(k\alpha) \equiv (51, 11) \pmod{179} \equiv P_m$$

因此, A 藉由加上 $k\beta_B$ 來隱藏訊息 P_m 。除了 A 之外沒人知道 k 的值, 所以即使 β_B 是公開的鑰匙, 也沒人能移除隱藏用的 $k\beta_B$ 。

7 橢圓曲線版的數位簽署

ElGamal 密碼系統是專門為簽署而設計的。其不同於 RSA 的一個特色就是對任何的一個信息有各種不同的簽署法。由於橢圓曲線能運用於 ElGamal 密碼系統中, 相對之下, 那橢圓曲線一樣也能運用於 ElGamal 數位簽署中。

令 $E: y^2 \equiv x^3 + ax + b \pmod{p}$ 為一橢圓曲線, 在其上選取一秩 (order) 為 $n \in \mathbb{N}$ 的點 $\alpha = (x, y)$, 並將 α 及 $E_p(a, b)$ 對所有密碼系統的參與者而言都是公開的。假設 A 想要利用橢圓曲線來簽署一份文件 m , 首先他選取一秘密隨機整數 a , 且 a 必須落在區間 $[1, n-1]$ 裡, 並且計算一等式 $\beta \equiv a\alpha \pmod{p}$, 此 $\alpha, \beta \in E_p(a, b)$ 。則 β 為 A 的公開鑰匙, 而 a 是為秘密鑰匙。使用者 A 對此信息 m 加以簽署, 其步驟如下:

1. 選取一介於 1 與 n 之間之秘密整數 k , 使得 $\gcd(k, n) = 1$ 。
2. 計算 $\gamma \equiv k\alpha \equiv (x_1, y_1) \pmod{p}$ 。
3. 計算 $s \equiv k^{-1}(m - ax_1) \pmod{n}$ 。
4. 因此簽署為 (m, γ, s) 。

B 的驗證程序如下:

1. 下載 A 的公開鑰匙 (E_p, α, β) 。
2. 計算 $v_1 \equiv x_1\beta + s\gamma \pmod{p}$ 以及 $v_2 \equiv m\alpha \pmod{p}$ 。
3. 接受此為有效簽署 $\iff v_1 = v_2$ 。

例題:

考慮在模 179 之下的橢圓曲線

$$E: y^2 \equiv x^3 + 2x + 7 \pmod{179}$$

選取一個滿足 $E_{179}(2, 7)$ 上的點 $\alpha = (111, 11)$, 使得 $n * (111, 11) = \infty$, 其中 $n = 13$ 。使用者 A 選取隨機整數 $a = 12$, 且 $a \in (1, 13)$, 並計算 $\beta \equiv 12\alpha = (111, 168) \pmod{179}$, 此 $\alpha, \beta \in E_{179}(2, 7)$ 。因此 A 將 $((111, 11), (111, 168), E_{179}(2, 7))$ 公開。 A 對信息 $m = 5$ 簽署, 其步驟如下:

1. 選取隨機整數 $k = 11$, 使得 $\gcd(11, 13) = 1$ 。
2. 計算 $\gamma \equiv k\alpha \equiv (152, 26) \pmod{179}$
3. 計算 $s \equiv k^{-1}(m - ax_1) \equiv 6 \pmod{13}$
4. 因此簽署為 $(5, (152, 26), 6)$ 。

B 的驗證程序如下:

1. 下載 A 的公開鑰匙 $(E_{179}(2, 7), (111, 11), (111, 168))$ 。
2. 計算 $v_1 \equiv x_1\beta + s\gamma \equiv (164, 160) \pmod{179}$ 計算 $v_2 \equiv m\alpha \equiv (164, 160) \pmod{179}$
3. 因此得到 $v_1 = v_2$, 所以此簽署是有效的。

8 橢圓曲線改良版的 ElGamal 數位簽署

令 $E: y^2 \equiv x^3 + ax + b \pmod{p}$ 為一橢圓曲線, 在其上選取一秩 (order) 為 $n \in \mathbb{N}$ 的點 $\alpha = (x, y)$, 並將 α 及 $E_p(a, b)$ 對所有密碼系統的參與者而言都是公開的。假設 A 想要利用橢圓曲線來簽署一份文件 m , 首先他選取一秘密隨機整數 a , 且 a 必須落在區間 $[1, n-1]$ 裡, 並且計算一等式 $\beta \equiv a\alpha \pmod{p}$, 此 $\alpha, \beta \in E_p(a, b)$ 。則 β 為 A 的公開鑰匙, 而 a 是為秘密鑰匙。使用者 A 對此信息 m 加以簽署, 其步驟如下:

1. 選取一介於 1 與 n 之間之秘密整數 k , 使得 $\gcd(k, n) = 1$ 。
2. 計算 $\gamma \equiv k\alpha \equiv (x_1, y_1) \pmod{p}$ 。
3. 計算 $s \equiv a^{-1}(x_1k - m) \pmod{n}$ 。
4. 因此簽署為 (m, γ, s) 。

B 的驗證程序如下:

1. 下載 A 的公開鑰匙 (E_p, α, β) 。
2. 計算 $v_1 \equiv x_1\gamma - s\beta \pmod{p}$ 以及 $v_2 \equiv m\alpha \pmod{p}$ 。
3. 接受此為有效簽署 $\iff v_1 = v_2$ 。

例題:

考慮在模 179 之下的橢圓曲線

$$E: y^2 \equiv x^3 + 2x + 7 \pmod{179}$$

選取一個滿足 $E_{179}(2, 7)$ 上的點 $\alpha = (111, 11)$, 使得 $n * (111, 11) = \infty$, 其中 $n = 13$ 。使用者 A 選取隨機整數 $a = 12$, 且 $a \in (1, 13)$ 。並計算 $\beta \equiv 12\alpha = (111, 168) \pmod{179}$, 此 $\alpha, \beta \in E_{179}(2, 7)$ 。因此 A 將 $((111, 11), (111, 168), E_{179}(2, 7))$ 公開。 A 對信息 $m = 5$ 簽署, 其步驟如下:

1. 選取隨機整數 $k = 11$, 使得 $\gcd(11, 13) = 1$ 。
2. 計算 $\gamma \equiv k\alpha \equiv (152, 26) \pmod{179}$
3. 計算 $s \equiv a^{-1}(x_1k - m) \equiv 10 \pmod{13}$
4. 因此簽署為 $(5, (152, 26), 10)$ 。

B 的驗證程序如下:

1. 下載 A 的公開鑰匙 $(E_{179}(2, 7), (111, 11), (111, 168))$ 。
2. 計算 $v_1 \equiv x_1\gamma - s\beta \equiv (164, 160) \pmod{179}$
計算 $v_2 \equiv m\alpha \equiv (164, 160) \pmod{179}$
3. 因此得到 $v_1 = v_2$, 所以此簽署是有效的。

9 同時達到秘密通訊和數位簽署

令 $E: y^2 \equiv x^3 + ax + b \pmod{p}$ 為一橢圓曲線, 在其上選取一秩 (order) 為 $n \in \mathbb{N}$ 的點 $\alpha = (x, y)$, 並將 α 及 $E_p(a, b)$ 對所有密碼系統的參與者而言都是公開的。

9.1 系統參數相同時

使用者 A 與 B 其系統參數 (p, α) 相同, 個人私密鑰匙求法如下:

1. A 選擇一小於 n 的整數 a_A , 此 a_A 為 A 的私密鑰匙, 然後 A 產生一公開鑰匙 $\beta_A \equiv a_A \alpha \pmod{p}$; 公開鑰匙為 $E_p(a, b)$ 上的一點。
2. B 同樣地選擇一私密鑰匙 a_B , 並且計算其公開鑰匙 $\beta_B \equiv a_B \alpha \pmod{p}$ 。
3. A 生成密鑰 $K \equiv a_A \beta_B \pmod{p}$, B 生成密鑰 $K \equiv a_B \beta_A \pmod{p}$ 。

步驟 3 的兩個運算會產生相同的結果, 因為

$$a_A \times \beta_B \equiv a_A \times (a_B \times \alpha) \equiv a_B \times (a_A \times \alpha) \equiv a_B \times \beta_A \pmod{p}$$

若 A 欲秘密傳送明文 m ($1 \leq m \leq p-1$), 並且同時對 m 做簽署, 然後傳送給 B 。其進行步驟如下: 使用者 A 首先對信息 m 加密, 得到密文 $C = \{\gamma, \delta\}$ 。然後再對密文 C 加以簽署, 得到簽署文 $S = \{x_1, s\}$ 。

1. A 任選一介於 1 及 n 之間的整數 k , 使得 $\gcd(k, n) = 1$ 。
2. 將信息 m 轉換成橢圓曲線上的點 P_m 。
3. 加密:

$$\begin{aligned} \gamma &\equiv k\alpha \pmod{p} \\ \delta &\equiv P_m + k\beta_B \pmod{p} \end{aligned}$$
4. 簽署:

$$\begin{aligned} \gamma &\equiv k\alpha \equiv (x_1, y_1) \pmod{p} \\ s &\equiv k^{-1}(m - a_A x_1) \pmod{n} \end{aligned}$$

B 收到 $\{C, S\}$ 後, 先進行解密的動作, 以求得信息 m ; 然後再執行驗證, 確定是否為 A 傳送過來的。

1. 解密: $P_m \equiv \delta - a_B \gamma \pmod{p}$
2. 將此橢圓曲線上的點 P_m 轉換成原來的信息 m 。
3. 驗證:

$$\begin{aligned} v_1 &\equiv x_1 \beta_A + s \gamma \pmod{p} \\ v_2 &\equiv m \alpha \pmod{p} \end{aligned}$$

例題：

考慮在模 179 之下的橢圓曲線

$$E : y^2 \equiv x^3 + 2x + 7 \pmod{179}$$

並選取一個滿足 $E_{179}(2, 7)$ 上的點 $\alpha = (111, 11)$, 使得 $n(111, 11) = \infty$, 其中 $n = 13$, 並將 $(111, 11)$ 及 $E_{179}(2, 7)$ 公開。使用者 A 的系統參數為 $(179, (111, 11))$, 私密鑰匙 $a_A = 12$, 其公開鑰匙為

$$\beta_A \equiv 12 * (111, 11) \equiv (111, 168) \pmod{179}$$

使用者 B 的系統參數為 $(179, (111, 11))$, 私密鑰匙 $a_B = 9$, 其公開鑰匙為

$$\beta_B \equiv 9 * (111, 11) \equiv (20, 23) \pmod{179}$$

若 A 要傳送信息 m , 並同時對 m 做簽署, 然後傳送給 B 。其進行步驟如下: A 的加密及簽署:

1. 選取一整數 $k = 11$, 使得 $\gcd(11, 13) = 1$ 。
2. 欲傳送信息 $m = 5$, 所以選擇 $K = 10$ 。可以成功的將 m 轉換成 $x = 5 * 10 + 1 = 51$, $y = 11$ 的點為 $P_m = (51, 11)$ 。
3. 加密: 計算 $\gamma \equiv k\alpha \equiv (152, 26) \pmod{179}$ 計算 $\delta \equiv P_m + k\beta_B \equiv (156, 18) \pmod{179}$
4. 簽署: 計算 $\gamma \equiv k\alpha \equiv (156, 26) \pmod{179}$ 計算 $s \equiv k^{-1}(m - a_A x_1) \equiv 6 \pmod{13}$

因此密文 $C = \{(152, 26), (156, 18)\}$, 簽署文 $S = \{152, 6\}$ 。 B 收到 $\{C, S\}$ 後進行解密及驗證:

1. 解密: 計算 $\delta - a_B \gamma \equiv (51, 11) \pmod{179} \equiv P_m$
2. 取其點 P_m 為中的 x 座標 51, 得 $[\frac{51}{11}] = 5$ 為原來的信息 m 。
3. 驗證: 計算 $x_1 \beta_A + s \gamma \equiv (164, 160) \pmod{179} \equiv v_1$ 計算 $m \alpha \equiv (164, 160) \pmod{179} \equiv v_2$
4. 因此得到 $v_1 = v_2$, 所以此簽署是有效的。

9.2 系統參數不相同時

使用者 A 與 B 其系統參數分別為 (p_A, α_A) 及 (p_B, α_B) , 個人私密鑰匙分別為 a_A 及 a_B , 個人公開鑰匙分別為 $\beta_A \equiv a_A \alpha_A \pmod{p_A}$ 及 $\beta_B \equiv a_B \alpha_B \pmod{p_B}$ 。

若 A 欲秘密傳送信息 $m (1 \leq m \leq p_B - 1)$, 並且同時對 m 做簽署, 然後傳送給 B 。首先 A 必須選取一橢圓曲線 $E : y^2 \equiv x^3 + ax + b \pmod{p_A}$, 並在其上選取一秩 (order) 為 $n \in \mathbb{N}$ 的點 $\alpha_A = (x, y)$, 並將 $\alpha_A = (x, y)$ 及 $E_{p_A}(a, b)$ 公開。其進行的步驟如下: 使用者 A 對信息 m 加密, 得到密文 $C = \{\gamma, \delta\}$ 。然後再對密文 C 加以簽署, 得到簽署文 $S = \{\gamma_A, \delta\}$ 。

1. A 任選一整數 k , 使得 $\gcd(k, n) = 1$ 。

2. 將信息 m 轉換成橢圓曲線上的點 P_m 。

$$3. \text{ 加密: } \gamma \equiv k\alpha_B \pmod{p_B} \quad \delta \equiv P_m + k\beta_B \pmod{p_B} \quad (4.1)$$

$$4. \text{ 簽署: } \gamma_A \equiv k\alpha_A \equiv (x_1, y_1) \pmod{p_A} \quad s \equiv k^{-1}(m - a_A x_1) \pmod{n} \quad (4.2)$$

B 收到 $\{C, S\}$ 後, 先進行解密的動作, 以求得信息 m ; 然後再執行驗證, 確定是否為 A 傳送過來的。

$$1. \text{ 解密: } P_m \equiv \delta - a_B \gamma \pmod{p_B} \quad (4.3)$$

2. 將此橢圓曲線上的點 P_m 轉換成原來的信息 m 。

3. 驗證:

$$v_1 \equiv x_1 \beta_A + s \gamma_A \pmod{p_A} \quad (4.4)$$

$$v_2 \equiv m \alpha_A \pmod{p_A} \quad (4.5)$$

10 Reblocking 問題的討論

若先執行加密再簽署時, 因為 A 和 B 之系統參數不同, 分別為 p_A 和 p_B , 所以有可能造成 Reblocking 問題。

1. 當 $p_B < p_A$ 時, 在解密時因 (4.1) 式解密出來 (4.3) 式的 m 和原來信息

(a) 當 $p_A > n$ 時,

i 若 $n > p_B$, 則 (4.1) 式和 (4.2) 式中的 m 相同。

ii 若 $n < p_B$, 則 (4.1) 式和 (4.2) 式中的 m 相同。

因為在 (4.2) 式中的 m 和 (4.1) 式中的 m 不相同, 之間相差了 n 倍, 由於一秩 (*order*) 為 $n \in \mathbb{N}$ 的點 α_A 會變成單位元數。因此, 在 (4.4) 式和 (4.5) 式中可知 v_1 和 v_2 之間只差 n 倍, 所以不會產生 Reblocking 的問題。

(b) 當 $n > p_A$ (i.e. $n > p_B$) 時, 則 (4.1) 式和 (4.2) 式中的 m 相同。

因此由 (a), (b) 可得 (4.1) 式解密出來的信息 m 和 (4.2) 式中的 m 相同, 所以在驗證時 (4.4) 式和 (4.5) 式等號會相等 (因為 $a_A x_1 + ks \equiv m \pmod{n}$), 因此不會造成 Reblocking。 (4.1) 式中的 m 相同, 所以不會造成 Reblocking。

2. 當 $p_B > p_A$ 時, 在解密時因為 (4.1) 式所解出來 (4.3) 式的 m 和原來 (4.1) 式中的信息 m 相同, 所以不會造成 Reblocking。但驗證時因 $p_B > p_A$ 時, 則

(a) 當 $p_A > n$ (i.e. $p_B > n$), 若 $m > n$ 則 (4.2) 式中的 m 和 (4.1) 式中的 m 會不相同, 之間相差了 n 倍, 由於一秩 (*order*) 為 $n \in \mathbb{N}$ 的點 α_A , 會變成單位元素。因此, 在 (4.4) 式和 (4.5) 式中可知 v_1 和 v_2 之間只差 n 倍, 所以不會產生 Reblocking 的問題。

(b) 當 $n > p_A$ 時,

- i 若 n 也大於 p_B (i.e. $n > p_B$), 則 (4.1) 式和 (4.2) 式中的 m 相同。
- ii 若 $n < p_B$ (i.e. $p_B > n$), 則 (4.2) 式中的 m 和 (4.1) 式中的 m 不相同, 之間相差了 n 倍, 由於一秩 (order) 為 $n \in \mathbb{N}$ 的點 α_A , 會變成單位元素。因此, 在 (4.4) 式和 (4.5) 式中可知 v_1 和 v_2 之間只差 n 倍, 所以不會產生 Reblocking 的問題。

因此由 (a), (b) 可得 (4.1) 式解密出來的信息 m 和 (4.2) 式中的 m 相同, 所以在驗證時 (4.4) 式和 (4.5) 式等號會相等 (因為 $a_A x_1 + ks \equiv m \pmod{n}$), 因此不會造成 Reblocking。由上可知雖然 p_A , p_B 不同, 但並不會影響其解密和驗證的過程。

例題 1: $P_A > P_B$

使用者 A 的系統參數為 $(191, (125, 5))$, 私密鑰匙 $a_A = 12$, 其公開鑰匙為 $\beta_A \equiv 12 * (125, 5) \equiv (182, 62) \pmod{191}$ 。使用者 B 的系統參數為 $(179, (111, 11))$, 私密鑰匙 $a_B = 9$, 其公開鑰匙為 $\beta_B \equiv 9 * (111, 11) \equiv (20, 23) \pmod{179}$ 。若 A 要傳送信息 m , 並同時對 m 做簽署, 然後傳送給 B 。首先 A 考慮在模 191 之下的橢圓曲線

$$E: y^2 \equiv x^3 + 2x + 7 \pmod{191}$$

並選取一個滿足 $E_{191}(2, 7)$ 上的點 $\alpha_A = (125, 5)$, 使得 $n(125, 5) = \infty$, 其中 $n = 96$, 並將 $(125, 5)$ 及 $E_{191}(2, 7)$ 公開。其進行步驟如下:

A 的加密及簽署:

1. 選取一整數 $k = 11$, 使得 $\gcd(11, 96) = 1$ 。
2. 欲傳送信息 $m = 5$, 所以選擇 $K = 10$ 。可以成功的將 m 轉換成爲 $x = 5 * 10 + 1 = 51$, $y = 11$ 的點爲 $P_m = (51, 11)$ 。
3. 加密:
計算 $\gamma \equiv k\alpha_B \equiv (152, 26) \pmod{179}$
計算 $\delta \equiv P_m + k\beta_B \equiv (156, 18) \pmod{179}$
4. 簽署:
計算 $\gamma_A \equiv k\alpha_A \equiv (123, 4) \pmod{191}$
計算 $s \equiv k^{-1}(m - a_A x_1) \equiv 67 \pmod{96}$

因此密文 $C = \{(152, 26), (156, 18)\}$, 簽署文 $S = \{(123, 4), 67\}$ 。 B 收到 $\{C, S\}$ 後進行解密及驗證:

1. 解密: 計算 $\delta - a_B \gamma \equiv (51, 11) \pmod{179} \equiv P_m$
2. 取其點 P_m 爲中的 x 座標 51, 得 $[\frac{51}{11}] = 5$ 爲原來的信息 m 。
3. 驗證:
計算 $x_1 \beta_A + s \gamma_A \equiv (43, 12) \pmod{191} \equiv v_1$
計算 $m \alpha_A \equiv (43, 12) \pmod{191} \equiv v_2$

4. 因此得到 $v_1 = v_2$, 所以此簽署是有效的。

例題 2: $P_B > P_A$

使用者 A 的系統參數為 $(179, (111, 11))$, 私密鑰匙 $a_A = 12$, 其公開鑰匙為 $\beta_A \equiv 12 * (111, 11) \equiv (111, 168) \pmod{179}$ 。使用者 B 的系統參數為 $(191, (125, 5))$, 私密鑰匙 $a_B = 9$, 其公開鑰匙為 $\beta_B \equiv 9 * (125, 5) \equiv (190, 189) \pmod{191}$ 。若 A 要傳送信息 m , 並同時對 m 做簽署, 然後傳送給 B 。首先 A 考慮在模 179 之下的橢圓曲線

$$E: y^2 \equiv x^3 + 2x + 7 \pmod{179}$$

並選取一個滿足 $E_{179}(2, 7)$ 上的點 $\alpha_A = (111, 11)$, 使得 $n(111, 11) = \infty$, 其中 $n = 13$, 並將 $(111, 11)$ 及 $E_{179}(2, 7)$ 公開。其進行步驟如下:

A 的加密及簽署:

1. 選取一整數 $k = 11$, 使得 $\gcd(11, 13) = 1$ 。
2. 欲傳送信息 $m = 5$, 所以選擇 $K = 10$ 。可以成功的將 m 轉換成爲 $x = 5 * 10 + 4 = 54$, $y = 2$ 的點爲 $P_m = (54, 2)$ 。
3. 加密:
計算 $\gamma \equiv k\alpha_B \equiv (123, 4) \pmod{191}$
計算 $\delta \equiv P_m + k\beta_B \equiv (102, 37) \pmod{191}$
4. 簽署:
計算 $\gamma_A \equiv k\alpha_A \equiv (152, 26) \pmod{179}$
計算 $s \equiv k^{-1}(m - a_A x_1) \equiv 6 \pmod{13}$

因此密文 $C = \{(123, 4), (102, 37)\}$, 簽署文 $S = \{(152, 26), 6\}$ 。 B 收到 $\{C, S\}$ 後進行解密及驗證:

1. 解密: 計算 $\delta - a_B \gamma \equiv (54, 2) \pmod{191} \equiv P_m$
2. 取其點 P_m 爲中的 x 座標 54, 得 $[\frac{54}{10}] = 5$ 爲原來的信息 m 。
3. 驗證:
計算 $x_1 \beta_A + s \gamma_A \equiv (164, 160) \pmod{179} \equiv v_1$
計算 $m \alpha_A \equiv (164, 160) \pmod{179} \equiv v_2$
4. 因此得到 $v_1 = v_2$, 所以此簽署是有效的。

11 Mathematica 的指令及程式

11.1 Mathematica 指令

在 Mathematica 中有兩個指令, 說明如下:

- *addell* $[\{x_1, y_1\}, \{x_2, y_2\}, a, b, n]$

計算在模 p 之下橢圓曲線

$$E : y^2 \equiv x^3 + ax + b \pmod{n}$$

上兩點 (x_1, y_1) 與 (x_2, y_2) 之和。所有的數 $x_1, x_2, y_1, y_2, a, b, n$ 都是整數。若 n 為合成數而計算兩點與之和時得求某個數在模 n 之下的乘法反元素與 n 的最大公因數既不是 1 也不是 n , 則輸出的東西為此最大公因數而非兩點之和。

- *multell* $[\{x, y\}, m, a, b, n]$

列舉在模 n 之下橢圓曲線

$$E : y^2 \equiv x^3 + ax + b \pmod{n}$$

上一點 $P = (x, y)$ 的倍數: $P, 2P, 3P, \dots, mP$ 。若需要求某個數在模 n 之下的乘法反元素且此數與 n 的最大公因數既不是 1 也不是 n , 則整個計算停止但輸出此最大公因數。這個指令可用來分解大約是 8 位數的整數, 所用的值大約 100: 當然有可能需要是幾條不同的橢圓曲線。

References

- [1] Elgamal, T. (1985), "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *Advances in cryptology : Proceedings of CRYPTO '84*, Springer-Verlag, 10-18. Also appeared in *IEEE Transactions on Information Theory*, **31**, 469-472.
- [2] Douglas R. Stinson (1996), "Cryptography Theory and Practice".
- [3] Miller, V. (1986), "Use of elliptic curves in cryptography", *Lecture Notes in computer science*, **218** 417-426. (Advances in Cryptology-CRYPTO'85).
- [4] Koblitz, N. (1987), "Elliptic Curve Cryptosystem", *Math. Comp.* **48**, 203-209.
- [5] Lenstra, H. W. Jr. (1987), "Factoring integers with elliptic curves", *Annals of Math*, **2** 126, 649-673.
- [6] James K. Strayer (1994), "Elementary Number Theory".
- [7] 賴溪松, 韓亮, 張真誠 (1995), "近代密碼學及其應用".
- [8] Silverman, Joseph H./Tate, Jhon, "Rational Points on Elliptic Curves".
- [9] 顏嵩銘 (1994), "公開金匙密碼系統之設計與運用法" 國立成功大學電機工程研究所博士論文.

ElGamal to Construct An Elliptic Curves Version of Digital Signature

Wen-Yi Lin* Yuan-Yuan Shen

Abstract

In this thesis, we are concerned with the elliptic curves digital signature and synchronize to the encryption and digital signature. In this research, Mention the discussion about ElGamal cryptosystem and digital signature at first, then talk about elliptic curves cryptosystem. Finally, we have the concept from ElGamal to construct an elliptic curves version of digital signature.

* Department of mathematics, Tunghai University